

**652.239-70**

Definitions for purposes of Section 136 determinations of eligibility—

*Assets* means tangible and intangible things of value conveyed or made available to the joint venture by the co-venturers. To be qualified for U.S. preference, 51 percent of the assets of the joint venture must be owned by the U.S. person co-venturer(s).

*Joint venture* means a formal or de facto association of two or more persons or entities to carry out a single business enterprise for profit, for which purpose they combine their property, money, effects, skills, and knowledge. To be acceptable, all members of a joint venture must be jointly and severally liable for full performance and resolution of matters arising out of the contract.

*Question 8(a)*: The prospective offeror is is not a joint venture.

*Question 8(b)*: If the prospective offeror is a joint venture, the U.S. person participant is:

\_\_\_\_\_  
(name)

\_\_\_\_\_  
(address)

*Question 8(c)*: If the prospective offeror is a joint venture, the names and countries of citizenship for all co-venturers are as follows:

\_\_\_\_\_  
(name)

\_\_\_\_\_  
(citizenship)

\_\_\_\_\_  
(name)

\_\_\_\_\_  
(citizenship)

\_\_\_\_\_  
(name)

\_\_\_\_\_  
(citizenship)

*Question 8(d)*: If the prospective offeror is a joint venture, the U.S. person will own at least 51 percent of the assets of the joint venture.

I so certify: (name) \_\_\_\_\_

\_\_\_\_\_  
(position)

\_\_\_\_\_  
(title)

(e) *Signature*: By signing this document, the offeror indicates that to the best of his or her knowledge, all of the representations and certifications provided in response to the questions contained in this Statement of Qualifications are accurate, current, and complete and that the offeror is aware of the penalty prescribed in 18 U.S.C. 1001 for making false statements.

(End of provision)

[69 FR 19343, Apr. 13, 2004, as amended at 76 FR 20251, Apr. 12, 2011]

**48 CFR Ch. 6 (10-1-11 Edition)**

**652.239-70 Information Technology Security Plan and Accreditation.**

As prescribed in 639.107-70(a), insert the following provision:

**INFORMATION TECHNOLOGY SECURITY PLAN  
AND ACCREDITATION (SEP 2007)**

All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and accreditation requirements as required by the clause at 652.239-71, Security Requirements for Unclassified Information Technology Resources.

(End of provision)

[72 FR 51569, Sept. 10, 2007]

**652.239-71 Security Requirements for Unclassified Information Technology Resources.**

As prescribed in 639.107-70(b), insert the following clause:

**SECURITY REQUIREMENTS FOR UNCLASSIFIED  
INFORMATION TECHNOLOGY RESOURCES (SEP  
2007)**

(a) *General*. The Contractor shall be responsible for information technology (IT) security, based on Department of State (DOS) risk assessments, for all systems connected to a Department of State (DOS) network or operated by the Contractor for DOS, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to DOS's information that directly supports the mission of DOS. The term "information technology", as used in this clause, means any equipment, including telecommunications equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes both major applications and general support systems as defined by OMB Circular A-130. Examples of tasks that require security provisions include:

(1) Hosting of DOS e-Government sites or other IT operations;

(2) Acquisition, transmission or analysis of data owned by DOS with significant replacement cost should the Contractor's copy be corrupted; and

(3) Access to DOS general support systems/major applications at a level beyond that granted the general public; e.g., bypassing a firewall.

(b) *IT Security Plan*. The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe

the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with applicable Federal laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and DOS policies and procedures, as they may be amended from time to time during the term of this contract that include, but are not limited to:

(1) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;

(2) National Institute of Standards and Technology (NIST) Guidelines (see NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Technology Systems (<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>)); and

(3) Department of State information security sections of the Foreign Affairs Manual (FAM) and Foreign Affairs Handbook (FAH) (<http://foia.state.gov/Regs/Search.asp>), specifically:

- (i) 12 FAM 230, Personnel Security;
- (ii) 12 FAM 500, Information Security (sections 540, 570, and 590);
- (iii) 12 FAM 600, Information Security Technology (section 620, and portions of 650);
- (iv) 5 FAM 1060, Information Assurance Management; and
- (v) 5 FAH 11, Information Assurance Handbook.

(c) *Submittal of IT Security Plan.* Within 30 days after contract award, the Contractor shall submit the IT Security Plan to the Contracting Officer and Contracting Officer's Representative (COR) for acceptance. This plan shall be consistent with and further detail the approach contained in the contractor's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as accepted by the Contracting Officer and COR, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

(d) *Accreditation.* Within six (6) months after contract award, the Contractor shall submit written proof of IT security accreditation for acceptance by the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation must be in accordance with NIST Special Publication 800-37. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity

of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The Contractor shall comply with the accepted accreditation documentation.

(e) *Annual verification.* On an annual basis, the Contractor shall submit verification to the Contracting Officer that the IT Security Plan remains valid.

(f) *Warning notices.* The Contractor shall ensure that the following banners are displayed on all DOS systems (both public and private) operated by the Contractor prior to allowing anyone access to the system:

Government Warning

\*\*WARNING\*\*WARNING\*\*WARNING\*\*

Unauthorized access is a violation of U.S. law and Department of State policy, and may result in criminal or administrative penalties. Users shall not access other user's or system files without proper authority. Absence of access controls IS NOT authorization for access! DOS information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized Department officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized Department officials. Use of this system constitutes consent to such monitoring.

\*\*WARNING\*\*WARNING\*\*WARNING\*\*

(g) *Privacy Act notification.* The Contractor shall ensure that the following banner is displayed on all DOS systems that contain Privacy Act information operated by the Contractor prior to allowing anyone access to the system:

This system contains information protected under the provisions of the Privacy Act of 1974 (Pub. L. 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to \$5,000, or both.

(h) *Privileged or limited privileged access.* Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for DOS or interconnected to a DOS network shall adhere to the specific contract security requirements contained within this contract and/or the Contract Security Classification Specification (DD Form 254).

## 652.242-70

(i) *Training.* The Contractor shall ensure that its employees performing under this contract receive annual IT security training in accordance with OMB circular A-130, FISMA, and NIST requirements, as they may be amended from time to time during the term of this contract, with a specific emphasis on rules of behavior.

(j) *Government access.* The Contractor shall afford the Government access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DOS data or to the function of information technology systems operated on behalf of DOS, and to preserve evidence of computer crime.

(k) *Subcontracts.* The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(l) *Notification regarding employees.* The Contractor shall immediately notify the Contracting Officer when an employee either begins or terminates employment when that employee has access to DOS information systems or data.

(m) *Termination.* Failure on the part of the Contractor to comply with the terms of this clause may result in termination of this contract.

(End of clause)

[72 FR 51569, Sept. 10, 2007]

## 652.242-70 Contracting Officer's Representative (COR).

As prescribed in 642.272(a), insert a clause substantially the same as follows:

### CONTRACTING OFFICER'S REPRESENTATIVE (COR) (AUG 1999)

(a) The Contracting Officer may designate in writing one or more Government employees, by name and position title, to take action for the Contracting Officer under this contract. Each designee shall be identified as a Contracting Officer's Representative (COR). Such designation(s) shall specify the scope and limitations of the authority so delegated; provided, that the designee shall not change the terms or conditions of the contract, unless the COR is a warranted Contracting Officer and this authority is delegated in the designation.

(b) The COR is [insert job title of COR].

## 48 CFR Ch. 6 (10-1-11 Edition)

(End of clause)

[53 FR 26177, July 11, 1988, as amended at 59 FR 66772, Dec. 28, 1994; 64 FR 43634, Aug. 11, 1999; 69 FR 19345, Apr. 13, 2004]

## 652.242-71 Notice of Shipments.

As prescribed in 642.1406-2-70(a), insert the following clause:

### NOTICE OF SHIPMENTS (JUL 1988)

At the time of delivery of supplies to a carrier for onward transportation, the Contractor shall give notice of prepaid shipment to the consignee establishment, and to such other persons as instructed by the Contracting Officer. If the Contractor has not received such instructions by 24 hours prior to the delivery time, the Contractor shall contact the Contracting Officer and request instructions from the Contracting Officer concerning the notice of shipment to be given.

(End of clause)

[53 FR 26177, July 11, 1988, as amended at 64 FR 43634, Aug. 11, 1999]

## 652.242-72 Shipping Instructions.

As prescribed in 642.1406-2-70(b), insert the following clause:

### SHIPPING INSTRUCTIONS (DEC 1994)

(a) Each packing box shall be of solid construction in accordance with best commercial practices and sufficiently strong in direct ratio to the weight of the contents to withstand excessively rough handling while in transit overseas. It shall be constructed of lumber that is well seasoned, reasonably sound, free from bad cross grain and from knots or knotholes that interfere with nailing or that occupy more than  $\frac{1}{8}$  of the width of the piece of lumber. Box shall be constructed with three-way corners and diagonal bracing. All nails shall be cement-coated, of correct size and properly spaced to avoid splitting or warping, and shall be driven into the grain of the wood. Dimension of lumber shall be in accordance with the following table, dependent upon the weight of the contents:

Weight of box and contents	Minimum dimensions of lumber for struts, frame members, and single diagonal braces
Up to 45 kg .....	19.05 × 57.15mm
46 to 113 kg .....	22.23 × 73.03mm
114 to 181 kg .....	22.23 × 98.43mm
182 to 272 kg .....	22.23 × 123.83mm or 25.4 × 98.43 mm

(b) Each box shall be lined with waterproof paper and shall be bound with 19.05mm" steel straps firmly stapled in position to prevent